GRC³

Protect Company Data with Strong Passwords

Passwords remain the first line of defense against hackers. Companies must establish robust cybersecurity policies to protect themselves from digital attacks.

Get assessment

How Hackers Steal Passwords

Phishing

Social engineering trick where hackers pose as legitimate sites to steal credentials.

Credential Stuffing

Testing stolen credentials against multiple accounts to find matches.

Brute Force

Systematically guessing passwords by testing all possible combinations

More Attack Techniques

Keylogging

Recording keyboard strokes to capture passwords, particularly effective for crypto wallets and bank accounts.

Local Discovery

Finding passwords written down in plain text where they can be easily seen.

Password Spraying

Testing common passwords like "123456" or "password" against user accounts until finding a match.

Extortion

Directly demanding users hand over credentials, often with threats if they don't comply.

5 Tips To Improve Password Security

01

Create Robust Passwords

Minimum 8 characters (preferably 14), mixing letter cases, numbers, and special characters.

02

Avoid Predictable Passwords

Don't use pet names, family members, birthplace, or school - anything discoverable on social media.

03

Use Passphrases

Easy to remember, meet character requirements, and harder to guess during brute force attacks.

04

Random Password Generators

Create complex passwords that are significantly harder to guess.

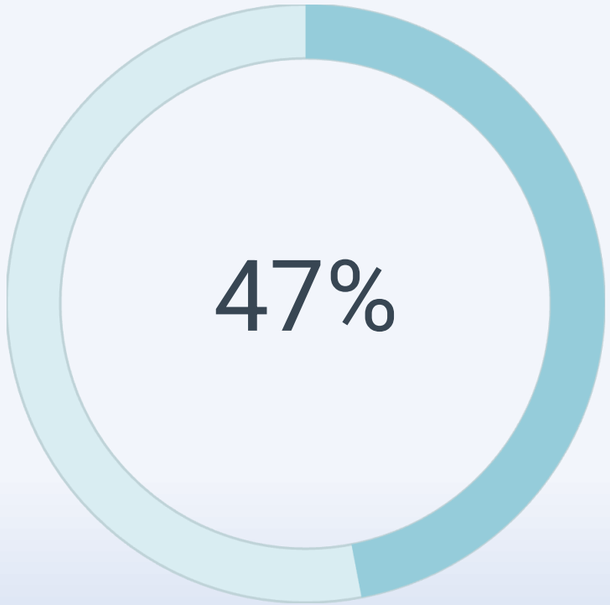
05

Implement Password Audits

Track compliance with security policies and identify weak access points.

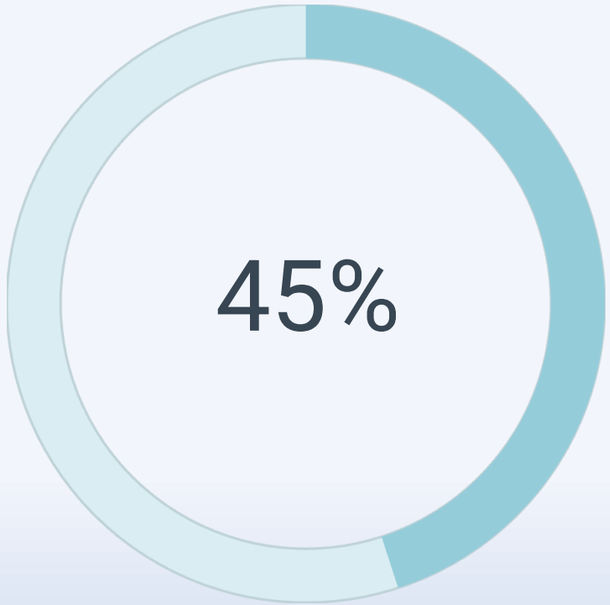
The Phishing Email Threat

Hackers pose as recognized authorities like banks or government departments, making emails appear legitimate. They demand sensitive information or redirect victims to fraudulent login forms that capture credentials.



Tech Industry

Employees who clicked phishing links



Banking & Finance

Employees who clicked phishing links

Protecting Against Phishing

Double-Check Email Sources

Always verify the sender before responding to requests for sensitive information.

Contact Administrators Directly

If an email claims to be from a higher-ranking individual, contact them directly to confirm authenticity.

Remember: Real Admins Don't Ask

Legitimate administrators have account access without needing to ask users for login details.

Don't assume tech-savvy departments don't need training. Quick email response expectations can lead to careless clicking.

Partner With GRC³ for DPDP Success

www.grc3.io (GRC Cube)

Contact:

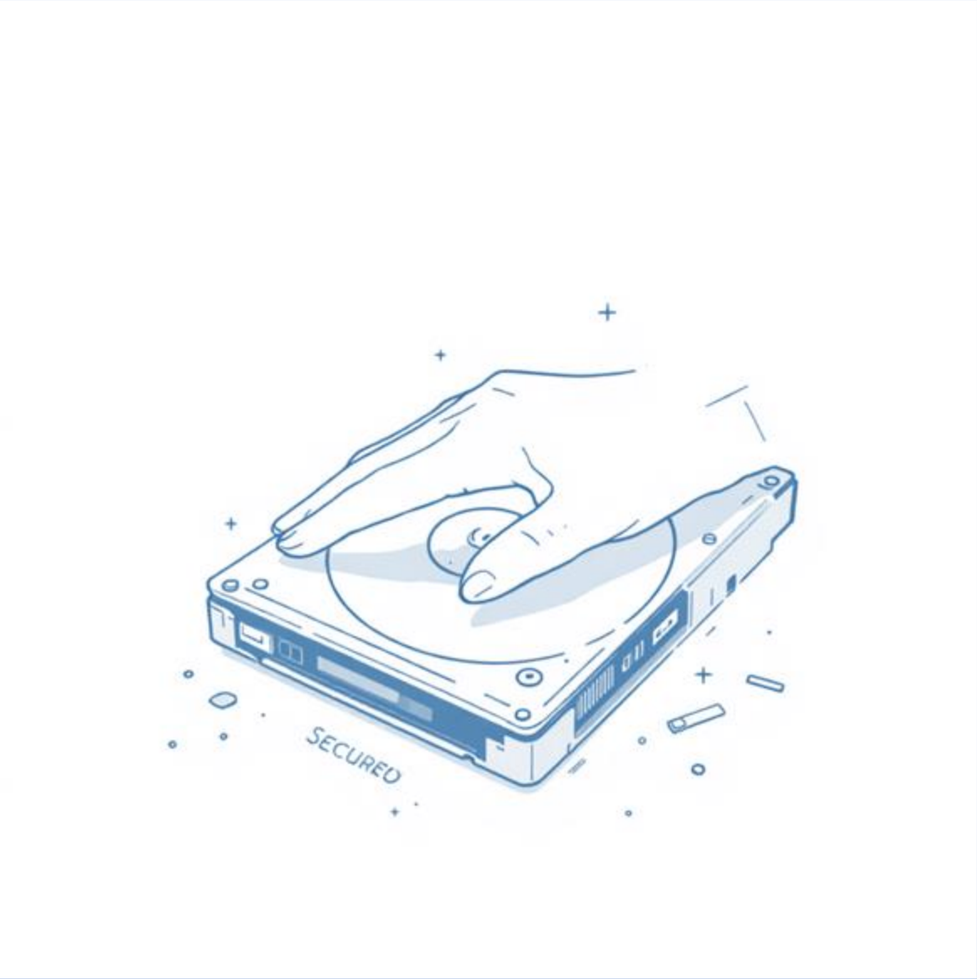
Nidhi P. - Nidhi.p@grc3.io / +91 9004735605

Mayuri B. - mayuri.b@grc3.io / +91 8097235523

Pooja D. - pooja.d@securetain.com

Charu P. - charu.pel@grc3.io

Data Wiping & Regular Password Changes



Data Wiping Old Equipment

Simple deletion isn't enough. Conduct full data wipes using specialized software to ensure no sensitive information or passwords remain on discharged IT equipment.

Regular Password Changes

Change passwords every **90 days** and passphrases every **180 days**

- Restrict password reuse (minimum 5 previous passwords)
- Set minimum password age: 3-7 days
- Prevent reverting to old passwords

Two-Step Authentication

Requires an additional device or verification point to validate credentials, confirming the real employee is attempting login.

1 2 3

Step 1

Enter password

Step 2

Receive verification code via email or text

Access Granted

Login successful after verification

Multi-factor authentication (MFA) apps generate one-time tokens that expire after 30 seconds, preventing hackers from guessing codes even if they know the password.

GRC³

Implementing A Robust Security Policy

Mandatory Training

Train all employees on password security during onboarding and provide ongoing education.

Password Managers

Invest in electronic password managers that encrypt credentials in a virtual vault, accessible with one master password.

Device Security

Inform employees about risks of accessing company data on both company and personal devices.

GRC³

Protect Your Organization

Data breaches cause severe reputational damage and hefty fines. Training employees on password security ensures everyone understands their responsibility for keeping credentials safe and secure.

Products & Features

Know More about our product

Products – Integrated Platform

All In One Solution

Compliance/Security	TPRM	Data Privacy	Internal Audit	IT Ops/Budgeting
Seamless Integration, Unmatched Efficiency ▪ 350+ Frameworks ▪ Algorithm-based mapping ▪ One-click delta visibility and task creation ▪ Global and ready to go	**Real Time Review & Response AI** ▪ Real-time review and unmatched speed ▪ Dashboard provides real-time visibility ▪ No more alert fatigue	**107 Privacy Laws Ready to Go** ▪ 107 Laws Ready Info Security and Consent/Rights Mgt out of box ▪ Ready reporting – DPIA	**Ease of Use and Saving on Time** ▪ Integrates with other Modules ▪ Able to use test results and validations from other modules	**Event, Incident, Breach Mgt , Change Mgt - out of box** ▪ Ease in integration with IT Ops ▪ Only tool with ready out of the box Breach, Findings Mgt,…

Competitors

Vendors - Provide a Maximum of 2 products

Compliance/Security	TPRM	Data Privacy	Internal Audit	IT Ops/Budgeting
▪ Couple of Vendors	▪ Couple of Vendors	▪ One Mainly	▪ One Mainly	▪ None for midsize

← Multiple providers, limited frameworks, duplication of work, lack of integration, risks falling through the gaps, adoption challenges, costs, inadequate reporting, no centralized dashboard, inadequate service management and findings documentation →

Why GRC³.io - The Fix: One Unified, AI-powered GRC Platform

Lower Total Operating Cost, Lower Risk, Continuous Trust. GRC³ is LIVE!

One Platform — Five Integrated, AI-Enabled and Proven to Scale.

5 Integrated Products	GRC3 Unique Feature	+ AI Advantage
Compliance / Frameworks	Unified engine supporting 350+ global frameworks. Offers real-time auto-mapping and change tracking.	Maps controls, builds smart workflows, and generates live policies.
Data Privacy	Pre-configured for 100+ global privacy laws. Provides centralized consent and rights management.	Accelerates compliance, consent tracking, and reporting.
Third Party Risk (TPRM)	Real-time vendor risk visibility with automated assessments and prioritization.	Closes gaps faster, auto-prioritizes risk, improves collaboration.
+ IT Operations	Cross-module linkage between breach, response, and control management	Connects incidents to controls, triages tasks, and forecasts risk.
Internal Audit	End-to-end audit automation and prioritization that shortens cycles.	Automates evidence, optimizes scope, maintains continuous audit readiness.

Benefits of GRC³ Platform

Accelerate Compliance
Build Trust
Scale with Confidence

As risk and regulatory demands surge, businesses need more than spreadsheets. GRC3 is a platform designed and developed by practitioners to **eliminate silos** between compliance, cybersecurity, internal audit, privacy, and vendor risk - enabling enterprises to **scale securely, accelerate revenue, and prove trust** enterprise-wide.

Learn More →

Get Your Free Maturity Assessment

Assess Compliance Maturity

Assess Privacy Maturity